INTERIM CHANGE 2003-1 TO AFI 33-211, COMMUNICATIONS SECURITY (COMSEC) USER REQUIREMENTS

31 OCTOBER 2003

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2003-1 (Attachment 8). Requires COMSEC managers to perform semiannual assessment and audits. Explains relief of accountability for the COMSEC Responsible Officer (CRO) and the users. Requires proof that the equipment is entered into the supply system before the material is issued to the CRO. Changes the requirement for keying material to be destroyed immediately after supersession instead of 12 hours after supersession. Requires exposed key tape segments be sealed in protective technology packaging or an opaque envelope. Deletes chopping as an approved method of destruction for COMSEC material. Adds new requirements for high security shredders and destruction methods of paper-mylar-paper key tapes. Provides more details on how to complete and retain Disposition Record Cards (DRC) with the local destruction report (SF-153). Changes retention of destruction certificates from 2 years to 3 years. Adds a Note about using another form of identification along with the Common Access Cards (CAC). Adds the Security Forces be notified in Task 2 of the Bomb Threat Task Cards.

★3.1.9. Perform semiannual assessments and audits of the CRO according to AFI 33-230, *Information Protection Assessment and Assistance Program* (to become *Information Assurance Assessment and Assistance Program*) and AFKAG 2, *Air Force COMSEC Accounting Manual*.

★3.3.21. Obtain relief of accountability from the COMSEC manager prior to leaving their current duty assignment. Ensure all COMSEC material is returned to the COMSEC manager and signed over to the new CRO.

★3.4.6. Obtain relief of accountability from the CRO prior to being relieved of duties as a COMSEC user. The CRO must ensure users are not signed for any COMSEC material.

★9.4. At a minimum the COMSEC records maintained by the CRO are operating instructions, emergency action plans, appointment letters, access list, requirements letter, AFCOMSEC Form 9, **Cryptographic Access Certificate (PA)**; AF Form 4160, **Information Assurance Assessment and Assistance Program (IAAP) Criteria**; AF Form 1109; **Visitor Register Log**; AFCOMSEC Form 16; AF Form 4168; DRC, destruction reports, hand receipts, waivers, EAP training, required reading, and semiannual assessments.

★13.2. Process requests for most COMSEC equipment through the Standard Base Supply System (SBSS). Proof of accountability that the equipment has been entered into the SBSS is required before COMSEC managers issue keying material to CROs. Requests for space and EKMS related equipments (i.e., AN/CYZ-10, KGR-96) are processed through the COMSEC account. Send a COMSEC material requirements letter to the COMSEC manager at the same time to make sure COMSEC material is on hand when required. Direct questions to your supporting COMSEC manager.

★16.2.2. When possible, issue keys electronically in a data transfer device (DTD). If physical key must be issued, issue key tape canisters in their entirety to include its

associated disposition record card or appropriate form. Before issuing key canisters, the CRO will remove and destroy all superseded material. Aircrew members must destroy any key tape segments removed from the canister immediately after supersession and record this destruction on the associated disposition record. Segments remaining in the canister need not be removed for destruction and will be returned to the issuing CRO.

★18.4. Verify personal clearance status from the currently approved security clearance verification roster, and that the person's need-to-know exists. CROs must review the authorized access list monthly to ensure its accuracy. Verify completion of the review by annotating the day, month, year and their initials on the list. Maintain only the most current access list. ***NOTE:*** The authorizing official (for FAA, Facility Manager) or CRO sign the authorized access list. Get security clearance information for civilian personnel (including DoD and civil agency contractors) from the base security forces office or other knowledgeable security offices.

★21.10. On an AFCOMSEC Form 16, inventory classified and, or certified (e.g., KGR-96, KOK-13, etc.) COMSEC equipment received from the COMSEC account through the CMCS. On a daily or shift-to-shift basis, account for operational cryptographic equipment (rack-mounted in the operating area) that contains accountable components or items as one complete unit without viewing the interior. List DTDs on the inventory, regardless if keyed or unkeyed.

★29.2. Destroy used keying material designated CRYPTO as soon as possible, but immediately after supersession. Under special circumstances (destruction device not operational, etc.), local commanders or authorizing officials can grant an extension of up to 24 hours. ***NOTE:*** Offices using COMSEC material that do not normally operate during weekends (normal or extended) must destroy superseded material on the first duty day after the weekend.

★29.2.2. Do not remove keytape segments stored in canisters until just before using or destroying them. Keep unused keytape segments in the keytape canister until needed or the canister's effective period ends. If you take out any keytape segments, destroy all superseded keytape segments immediately. Exposed key tape segments must be sealed in NSA protective technology packaging or an opaque envelope sealed in such a way that tampering would be obvious (i.e., writing the initial over the seal). Annotate the short title, ACN, segment, and quantity on the sealed envelope and store it with the canister and DRC. Use AFCOMSEC Form 21, AFCOMSEC Form 22A, AFCOMSEC Form 22B, or DRC to record the individual keytape segments destroyed. ***NOTES:*** (1) If additional copies of the same key segment remain in the canister, destroy the used segment immediately after keying the equipment. Keep the last copy of the key segment until it is superseded and then destroy it immediately after supersession. (2) If single-copy key is used, destroy key segments immediately after equipment rekeying if the circuit is very reliable. For unreliable circuits, single-copy segments may be kept for rekeying, but then destroy it immediately after supersession. Document unreliable circuits to the controlling authority with a letter, e-mail, or message and annotate the authority on the DRC. (3) Disposition records used for unclassified ALC-1, ALC-6, or ALC-7 keying material are UNCLASSIFIED FOR OFFICIAL USE ONLY when filled in.

★29.2.2.1. When making annotations on the disposition record (e.g., AFCOMSEC Form 22B, DRC, etc.), individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

★29.2.2.1.1. For partial canisters: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be "Z"d on the DRC.

★29.2.2.1.2. For entire canisters:

★29.2.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF-153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

★29.2.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

★29.2.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

★29.6. Destroy compromised material immediately after you receive disposition instructions or upon receipt of case closure from AFCA.

★30. Routine Destruction Methods. The authorized methods for routinely destroying paper COMSEC aids are pulverizing, high security crosscut shredding, burning, and pulping. Destroy nonpaper COMSEC aids authorized for routine destruction by pulverizing or chemically altering them. Consult the COMSEC manager for a list of NSA-approved paper destruction devices.

★30.1.2. When pulping or pulverizing paper COMSEC aids, break the material into bits no larger than five millimeters.

★30.1.3. Key tapes are paper-mylar-paper. The only approved methods for destroying key tapes are by a disintegrator, burning, or pulverizing. Do not place keying material in burn bags for destruction along with other classified waste.

★30.2. Non-Paper COMSEC Aids. Destroy the material so that no one can reconstruct it by physical, chemical, electrical, optical, or other means. The authorized methods of routinely destroying non-paper COMSEC aids are melting, pulverizing, and chemical alteration.

★32.1.1. Use the DRC provided to record destruction of each key setting. Destroy unused key, pages, tables, or day sheet, etc., when you load a current one or immediately after supersession.

★32.1.2. Provide a copy of all completed destruction records (SF 153) to the COMSEC account no later than the first duty day after the material supersession. The CRO will attach the completed DRCs to the applicable SF 153. These may be maintained by the CRO or the COMSEC account; it is the COMSEC Manager's choice. When the DRCs are attached the SF 153 becomes CONFIDENTIAL.

★32.1.4. For items issued to transient or deploying aircrews not returning to your location, file a copy of the signed, annotated receipt and keep it for 3 years after the yearly cutoff. Returning aircrews must immediately give unused material and DRC to their CRO.

★32.2.2. When the COMSEC manager directs, destroy the material, record destruction of classified documents on a SF 153, and keep the destruction certificate for 3 years according to AFMAN 37-139.

★59.2. Users positively identify all COMSEC assessors by comparing the identification card (DD Form 2, **Armed Forces Identification Card [Active, Reserve, and Retired]**, Common Access Card, or Air Force Form 354, **Civilian Identification Card**) with the assessment/audit message notice, TDY orders, or records the COMSEC manager provides. Sign them in on the Air Force Form 1109 or FAA Form 1600-8 (for FAA accounts). ***NOTE:*** Another form of ID may be needed with the CAC since SSNs are not listed on civilian or contractor CACs. Use a valid state driver license or a recent payroll statement as a second form of ID with the CAC.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-13, *The Paperwork Reduction Act of 1995*

CJCSI 3260.1, (S) *Policy Governing JCS Material* (U)

AFPD 33-2, *Information Protection*

AFI 31-209, *The Air Force Resource Protection Program*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-201, *Communications Security (COMSEC) (FOUO)*

AFI 33-210, *Cryptographic Access Program*

AFI 33-212, *Reporting COMSEC Deviations*

★AFI 33-230, *Information Protection Assessment and Assistance Program (*will become *Information Assurance Assessment and Assistance Program)*

AFI 33-275, *Controlled Cryptographic Items*

★AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 33-272, (S) *Classifying COMSEC and TEMPEST Information* (U) (will become *Classifying Information Assurance Information (U)*)

AFMAN 37-139, *Records Disposition Schedule*

AFDIR 33-303, *Compendium of Communications and Information Technology*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

★AFKAG-2, *Air Force COMSEC Accounting Manual*

AFSSM 4003, (C) *Emergency Destruction of Communications Security Equipment Elements* (U)

Abbreviations and Acronyms

ACN	Accounting Control Number
AFCA	Air Force Communications Agency
AFCOMSEC	Air Force Communications Security
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Manual
ALC	Accounting Legend Code
CAP	Cryptographic Access Program
CCI	Controlled Cryptographic Item
CIK	Crypto-Ignition Key
CJCSI	Chairman of the Joint Chief of Staff Instruction
CMCS	COMSEC Material Control System
CM^2	Computerized Management of COMSEC Material
CNLZ	COMSEC No-Lone Zone
COMSEC	Communications Security
CONUS	Continental United States
COR	Central Office of Record
CRO	COMSEC Responsible Officer
DRC	Disposition Record Card
DRU	Direct Reporting Unit
DTD	Data Transfer Device
EAP	Emergency Action Plan
EKMS	Electronic Key Management System

EOM	End of Month
FAA	Federal Aviation Administration
FOA	Field Operating Agency
GS	General Schedule
GSA	General Services Administration
IAAP	Information Assurance Assessment and Assistance Program
MAJCOM	Major Command
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OI	Operating Instruction
PAL	Permissive Action Link
PROM	Programmable Read-Only Memory
RON	Remain Overnight
SAS	Sealed Authenticator System
SBSS	Standard Base Supply System
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SSN	Social Security Account Number
STU	Secure Telephone Unit
TDY	Temporary Duty
TPI	Two-Person Integrity
UCM^2	Users Computerized Management of COMSEC Material
URL	Uniform Resource Locator

Terms

Authorizing Official The official who authorizes individuals to perform COMSEC responsibilities. At the wing level the staff directorate (two-letter personnel under the commander) is the authorizing official. At the group level and below the commander is the authorizing official.

COMSEC Aids COMSEC material, other than equipment or devices, that helps to secure telecommunications and is needed to produce, operate, or maintain COMSEC systems and their components. Some examples are COMSEC keying material (items such as codes, keytapes, keylists, authenticators, one-time pads, and so forth, marked CRYPTO), call sign or frequency systems, and supporting documentation such as operating and maintenance manuals.

COMSEC Manager Individual responsible for managing the COMSEC resources of a COMSEC account.

COMSEC Material An item that secures or authenticates telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware or software that holds or describes cryptographic logic, and other items for COMSEC functions.

COMSEC Material Control System (CMCS) The logistics system for distributing, controlling, and protecting COMSEC material. It consists of all COMSEC central offices of record (COR), cryptological depots, and COMSEC accounts.

COMSEC Operations COMSEC operations include distributing, safeguarding, destroying, and accounting for all COMSEC material at all administrative and operational COMSEC accounts and all COMSEC user locations.

COMSEC Responsible Officer (CRO) The individual within an office or area responsible for COMSEC material received from the CMCS.

COMSEC Users Individuals who have access to COMSEC material and must use and safeguard COMSEC material to perform their official duties.

Electronic Key Management System (EKMS) Interoperable collection of systems being developed by services and agencies of the U.S. Government to automate the planning, ordering, generation, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material.

Attachment 3

SAMPLE COMMUNICATIONS SECURITY REQUIREMENTS LETTER

(Unit Letterhead)

MEMORANDUM FOR COMSEC ACCOUNT_____ *(Date)*

FROM: (*Your unit office symbol*)

SUBJECT: COMSEC Requirements

1. COMSEC requirements for (*organization and office symbol*) are:

a. (*Enter the short title of documents and quantity needed.*)

b. (*If you request more copies of material you already have, give the number of copies you have and the new total you require*.)

c. (*Enter the date you need the material.*)

2. Authorization or Justification. (If you ask for new COMSEC material, include copies describing the use of the actual authority or justification request or excerpts detailing the material's use. Justification for all requirements, including existing needs, must be specific (for example: "HQ AFCA requires material in support of Operation Plan (OPLAN), JCS Exercise_____, and so forth" General statements, such as "to fulfill mission requirements" or "as directed by XYZ message 091234Z Jan 02," are not accepted by themselves; we need further justification.)

★3. Attached is proof that the equipment has been entered into the Standard Base Supply System according to AFMAN 23-110.

(*Signature Element of CRO*)

Attachment 5

SAMPLE -- COMMUNICATIONS SECURITY EMERGENCY ACTION PLAN

A5.1. Fire Task Cards.

EXAMPLE - Task Card #1:

-- Purpose. Provides for orderly evacuation of personnel and protection of COMSEC material within facilities using COMSEC aids and equipment in case of fire.

-- The senior person present implements the plan by issuing task cards. If a limited number of personnel are available to carry out each task, combine the tasks.

-- After the fire is out, inspect the safes for signs of entry or tampering and take a complete inventory of all COMSEC material.

-- If you find evidence of tampering or damage, thoroughly page check all COMSEC items.

-- If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately

EXAMPLE - Task Card #2.

-- Sound alarm and notify Fire Department, stating: **THIS IS** (*Rank/Name*)**, REPORTING A FIRE IN BUILDING _____, ROOM _____.**

-- Do not hang up the telephone until the fire dispatcher knows the location and has no questions.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #3.

-- Secure all COMSEC material (keytapes, keylists, code books, Data Transfer Device (DTD), and so forth), the STU-III keys, and all other classified material in the safe along with COMSEC inventories.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #4.

-- Fight any open fire, if possible, using available fire extinguishers.

-- Fire extinguisher(s) ___(*Type*)___ is/are located _____(*where*)_____.

EXAMPLE - Task Card #5.

-- Open and guard the door that gives fire department personnel greatest access to the fire.

-- Admit all firefighting personnel, including local national firefighters.

EXAMPLE - Task Card #6.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- Manager, COMSEC account _____ (duty hour phone number _____ and non-duty hour phone number _____).

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #7.

-- Take names of all Fire Fighters for inadvertent oath, if necessary.

-- Take inventory to ensure all material is present.

-- Report back to the senior person for further instructions.

A5.2. Natural Disaster Task Cards:

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC materials in the event of a natural disaster (e.g., flood, earthquake, hurricane, etc.).

-- For natural disasters that require evacuation of the facility or seriously impair its physical security, the senior person implements this plan by issuing the remaining task cards. If a limited number of personnel are available to carry out the tasks, combine the tasks.

-- After the emergency, inspect the safes for signs of entry or tampering, and completely inventory of all COMSEC material.

-- If you find evidence of tampering or damage, thoroughly page check all COMSEC items.

-- If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately.

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- If time and circumstances permit, destroy all superseded COMSEC material and annotate the destruction.

EXAMPLE - Task Card #4.

-- Secure all other COMSEC material (e.g., keytapes, keylists, code books, DTD, etc.), the STU-III keys, and classified material in the safe along with COMSEC inventories.

★A5.3. Bomb Threat Task Cards:

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC materials in the event of a bomb threat.

-- In the event of a bomb threat, the senior person implements the plan by issuing the remaining task cards. If a limited number of personnel are available to carry out the tasks, combine the tasks.

-- After the emergency, inspect the safes for signs of entry or tampering, and completely inventory all COMSEC material.

-- If you find evidence of tampering or damage, thoroughly page check all COMSEC items.

-- If items are damaged or missing, or you suspect unauthorized exposure, notify the COMSEC manager immediately.

EXAMPLE - Task Card #2.

-- Notify the Security Forces.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

EXAMPLE - Task Card #3.

-- Gather and secure all COMSEC material (keytapes, keylists, code books, DTD, etc.), the STU-III keys, and classified material in the safe along with the COMSEC inventories.

-- Leave the building and go to the designated assembly point located (enter location).

EXAMPLE - Task Card #4.

-- Conduct a search of the area and look for suspicious objects.

-- If found, guard the entrance and admit only authorized personnel until security police take over.

-- If not found, leave the building and go to the designated assembly point located (enter location).

A5.4. Emergency Evacuation Task Cards:

EXAMPLE - Task Card #1.

-- Purpose. To protect COMSEC material in facilities using COMSEC aids and equipment during emergency evacuation.

-- For emergencies that require evacuation of a facility or seriously impair its physical security, the senior member present distributes the remaining task cards and oversees the evacuation. If a limited number of personnel are available to carry out the tasks, combine the tasks.

-- After the emergency, completely inventory all COMSEC material.

-- If you suspect tampering or damage, thoroughly page check all COMSEC items.

-- If items are damaged or missing, or if you suspect unauthorized exposure, notify the COMSEC manager immediately.

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

EXAMPLE - Task Card #3.

-- If time permits, destroy all superseded COMSEC aids.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #4.

-- Gather all current material required for immediate secure communications, as well as the COMSEC inventory, and put them in a canvas bag.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #5.

-- Remove COMSEC aids in use from all COMSEC equipment and put them in a canvas bag.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #6.

-- Secure the facility as well as possible so forced entry will be obvious.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #7.

-- If you expect to evacuate for a short time, secure all other COMSEC items (including future COMSEC aids) in an approved storage container.

-- Put material required to maintain secure communications in a canvas bag.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #8.

-- Evacuate the material, under constant surveillance, preferably by authorized personnel, to the designated evacuation site and begin secure communications.

A5.5. Emergency Destruction Task Cards

A5.5.1. Phase I--Precautionary Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidelines for:

--- Destroying COMSEC material during emergencies resulting from natural, accidental, or hostile causes.

--- Reducing holdings as a precautionary measure.

--- Preventing their capture or compromise in an actual emergency or attack.

-- Personnel authorized to implement this plan:

--- Commander (applicable unit).

--- Commander (issuing COMSEC account unit).

--- Manager, COMSEC account.

--- CRO or alternate.

--- Senior member present.

-- After completing precautionary destruction, record all destruction on the preaddressed precautionary destruction letter and hand carry it to the COMSEC manager.

EXAMPLE - Task Card #2.

-- Contact the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #3.

-- Gather all COMSEC accounting records (i.e., inventories, destruction reports, hand receipts, etc.) and give them to the senior person present for safekeeping.

-- Gather the current month's inventory from the safe, take it to the incinerator room, and wait until someone brings material for you to destroy.

-- As you destroy each item, mark it off on the inventory form (AFCOMSEC Form 16).

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #4.

-- Go to the incinerator in Building _____ and fire it up.

-- The material for destruction is brought to you.

-- Place it in the incinerator as you receive it.

-- Tend the incinerator until all material is burned.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #5.

-- Gather all superseded COMSEC aids, using the attached Priority of Destruction list, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #6.

-- Gather all future COMSEC aids (those not scheduled to go into effect within the next 60 days), using the destruction priority listing, and place in canvas bags.

-- Take the bags to the incinerator for destruction.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #7.

-- Gather all administrative documents, files, training aids, and other material not required for continued operations and place in canvas bags.

-- Take the bags to the incinerator for destruction.

-- Report back to the senior person for further instructions.

A5.5.2. Phase II--Total Emergency Destruction Task Cards:

EXAMPLE - Task Card #1.

-- Purpose: To provide guidance for preventing capture or compromise of COMSEC material in an actual emergency or attack.

-- The commander of the applicable unit, the commander of the issuing COMSEC account, the COMSEC manager account number _____, the CRO or alternate, or the senior member present may implement this plan. They do this by distributing the remaining task cards and monitoring task completion.

-- After emergency destruction or as soon as possible if emergency destruction is not completed, record all destruction on the preaddressed emergency destruction letter and carry it to the COMSEC manager.

EXAMPLE - Task Card #2.

-- Notify the following personnel:

--- Commander (applicable unit).

--- CRO (applicable unit).

--- COMSEC manager.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #3.

-- Gather the current month's inventory from the safe, take it to the incinerator room, and wait until someone brings you material for destruction.

-- As you destroy each item, check it off on the inventory form (AFCOMSEC Form 16).

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #4.

-- Go to the incinerator in Building _____ and fire it up. Wait there until someone brings you material for destruction.

-- Place the material in the incinerator when you receive it.

-- Tend the incinerator until all the material is burned.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #5.

-- Declassify all COMSEC equipment by removing the key and zeroizing.

-- Gather all COMSEC aids using the destruction priority list and place it in canvas bags.

-- Take the bags to the incinerator for destruction.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #6.

-- Gather all current COMSEC aids, using the priority of destruction list, and place them in canvas bags.

-- Take the bags to the incinerator for destruction.

-- Report back to the senior person for further instructions.

EXAMPLE - Task Card #7.

-- Remove all classified and Controlled Cryptographic Item (CCI) boards from the COMSEC equipment, thoroughly smash them with a hammer or an ax, and scatter the pieces.

-- Document destruction on the COMSEC inventory (AFCOMSEC Form 16).

-- Write names of unlisted items on the back of the form.

-- Report back to the senior person for further instructions.

A5.6. Priority of Destruction. Include, as a minimum, the following elements in your priority of destruction documentation: priority, locations, short titles of material, and safe number.

A5.6.1. Keying Material.

A5.6.1.1. All superseded keying material and future editions of sealed authenticator system (SAS) and permissive action list (PAL) material:

A5.6.1.1.1. TOP SECRET (shared material ahead of point-to-point).

A5.6.1.1.2. SECRET (shared material ahead of point-to-point).

A5.6.1.1.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.2. All current keying material (zeroize all cryptographic equipment and remove and destroy current keylists and keytapes).

A5.6.1.2.1. TOP SECRET (shared information ahead of point-to-point).

A5.6.1.2.2. SECRET (shared information ahead of point-to-point).

A5.6.1.2.3. CONFIDENTIAL (shared information ahead of point-to-point).

A5.6.1.3. All future keylists, keytapes, codes, and authenticators scheduled to take effect within the next 30 days:

A5.6.1.3.1. TOP SECRET (shared information).

A5.6.1.3.2. SECRET (shared information).

A5.6.1.3.3. CONFIDENTIAL (shared information).

A5.6.1.4. All remaining future keying material.

A5.6.2. COMSEC Documents.

A5.6.2.1. Sensitive pages of cryptographic equipment maintenance manuals.

A5.6.2.2. Remaining classified documents.

A5.6.2.3. Classified COMSEC files.

A5.6.3. Cryptographic Equipment.

A5.6.3.1. Remove and destroy (time permitting), and list location.

A5.6.3.1.1. Readily removable classified and sensitive CCI elements.

A5.6.3.1.2. Remaining classified and sensitive CCI parts or components.

Attachment 7

HANDLING INSTRUCTIONS FOR ALL KEYTAPES

A7.1. Do not remove keytape segments until immediately prior to use or destruction. DO NOT REMOVE TAPE SEGMENTS FOR INVENTORY. If a tactical user requires more key than can be set or electrically stored in the crypto-equipment, the user may furnish additional key in electrical form in a common fill device or in hard copy form in a tape canister. Do not issue tape segments as extracts.

★**A7.2.** Maintain the applicable disposition record card (DRC) for each keytape canister. Retain completed DRC and attach it to the local destruction report (SF 153).

★A7.2.1. When making annotations on the disposition record (e.g., AFCOMSEC Form 22B, DRC, etc.), individuals will place date, signature or initial, in each applicable block. For Top Secret keytapes two initials are required for issue to validate that TPI procedures are being followed.

★A7.2.1.1. <u>For partial canisters</u>: If segments 1 through 10 are used within a canister and segments 11 through 31 remain at the end of the month and must be destroyed, the remainder of the canister may be "Z"d on the DRC.

★A7.2.1.2. <u>For entire canisters:</u>

★A7.2.1.2.1. If no segments were issued, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" – "No segments issued" and both the destruction official and witness will initial next to the statement. No DRC is required.

★A7.2.1.2.2. If all segments are loaded into a DTD, destroy the entire canister, complete an SF 153 only, annotate after the "Nothing Follows" "All segments loaded into DTD S/N XXXXXXXXX" and both the destruction official and witness will initial next to the statement. No DRC is required.

★A7.2.1.2.3. If all segments are loaded into a DTD and the segments need to be retained, (circuit must be unreliable and you must have something from the controlling authority stating to retain keying material) seal the segments in NSA protective packaging or an opaque envelope where tampering is evident. Superseded key must be destroyed during the month if the material locked in a safe is accessed during the month. Annotate the DRC the same as partial canisters.

A7.3. COMSEC managers may destroy segments of unissued tapes as they are superseded or may destroy unissued tapes as whole editions.

A7.4. Some key that is designated for off-the-air use (e.g., maintenance, test, classroom training, and demonstrations) has no prescribed cryptoperiod and may be used until no longer serviceable and then destroyed.

A7.5. Reproduction of associated tape is prohibited without the approval of the controlling authority.

A7.6. Notify the controlling authority immediately if the associated tape is lost, subjected to unauthorized viewing, or possibly compromised in any way. Report any incident according to AFI 33-212.

A7.7. Canister Disposition Instructions: Remove barcode stickers and destroy as classified trash. Once the key has been superseded and removed from the canister, destroy both large flat surfaces of the canister. The destruction of the canister requires that you follow the DESTRUCTION PROCEDURE below, and in addition, apply the proper SAFETY PROCEDURES at the time of destruction.

A7.8. Safety Procedures. An empty tape canister will shatter if fractured with a blunt instrument. To protect from possible injury due to flying fragments, place the canister inside a zip-lock plastic bag or similar sealable bag before beginning the destruction procedure. Wear protective eyewear during the destruction procedure to prevent injury.

A7.9. Destruction Procedure. Place the canister inside a zip-lock plastic bag or similar sealable bag, and set it down on a flat solid surface. Using a small head, 18 oz. ball peen hammer, fracture one face of the canister approximately 3/4" from the round edge, avoiding the exact center of the canister. Turn the canister over and repeat. Grab the bag by the edge and dispose of the canister and bag as UNCLASSIFIED trash.

A7.9.1. TO PUNCTURE: With a wide-blade screwdriver and hammer, puncture one flat side of the canister approximately 3/4" from the rounded edge, avoiding the exact center. Turn the canister over and repeat.

A7.9.2. TO SMASH: Place bagged canisters inside a canvas bag, or wrap loosely in a protective cloth, before smashing. Check to assure both flat sides are destroyed.

A7.10. Locally reproduce this instruction and provide a copy to each user issued key in canisters.